

PATENT ABSTRACTS OF JAPAN

A9

(11)Publication number : 2002-204228
(43)Date of publication of application : 19.07.2002

(51)Int.CI.

H04L 9/08
G06F 15/00
H04L 9/14

(21)Application number : 2000-400839

(71)Applicant : HAYASHI TOSHINORI
YAMADA YASUHIKO
KYO SENMEI
NAKAHARA YORIJI

(22)Date of filing : 28.12.2000

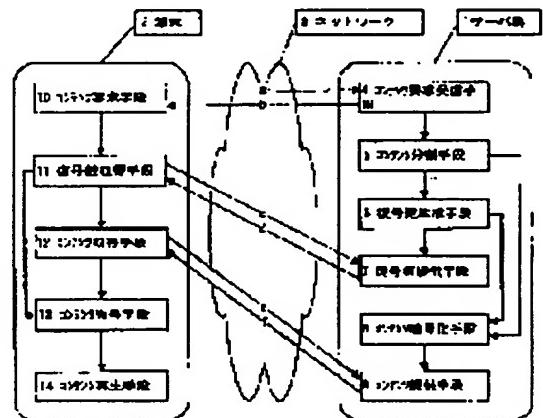
(72)Inventor : HAYASHI TOSHINORI
YAMADA YASUHIKO
KYO SENMEI
NAKAHARA YORIJI

(54) DEVICE AND METHOD FOR DISTRIBUTING CONTENTS, AND PROGRAM AND DEVICE FOR DOWNLOADING CONTENTS

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a method and a device for distribution of digital contents which enable prevention of illegal duplication and circulation of digital contents without spoiling the convenience for a legitimate user.

SOLUTION: The digital contents stored on a server are divided into two or more parts, which are each ciphered with different cipher keys and distributed to the user in the ciphered state and the cipher keys applicable to the distributed divided digital contents are distributed to the user.



LEGAL STATUS

[Date of request for examination] 30.01.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision]

THIS PAGE BLANK (USPS)

[of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

THIS PAGE BLANK (USPTO)

Japanese Publication for Unexamined Patent Application

No. 2002-204228/2002 (Tokukai 2002-204228)

A. Relevance of the above-identified Document

The following is a partial English translation of exemplary portions of non-English language information that may be relevant to the issue of patentability of the claims of the present application.

B. Translation of the Relevant Passages of the Document

See the attached English Abstract.

[DETAILED DESCRIPTION OF THE INVENTION]

[MEANS TO SOLVE THE PROBLEMS]

[0007]

More specifically, the present invention is to provide a digital content delivering method for delivering digital content to a user, the digital content stored in a server. The method is characterized in that the digital content is divided in two or more portions, which are encrypted with different encryption keys respectively; the encrypted portions of the digital content are delivered to the user; and decoding keys applicable to the portions of the digital content are delivered to the user. This method is characterized in that, for the encrypted and delivered portions of the content, the entire content is delivered by user repeating (i) the step of receiving transmission of

THIS PAGE BLANK (use . . .)

a portion of the content, (ii) the step of acquiring via a network, a decoding key at the same time when the user receives the transmission of the portion of the content, the decoding key corresponding to the encryption key, (iii) the step of decoding the portion of the content by using the decoding key, and (iv) deleting the portion of content and the decoding key.

THIS PAGE BLANK (USPTO)

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-204228

(P2002-204228A)

(43)公開日 平成14年7月19日 (2002.7.19)

(51)Int.Cl.⁷

H 04 L 9/08
G 06 F 15/00
H 04 L 9/14

識別記号

3 3 0

F I

G 06 F 15/00
H 04 L 9/00

テ-マ-ト⁷(参考)

3 3 0 Z 5 B 0 8 5
6 0 1 B 5 J 1 0 4
6 4 1

審査請求 未請求 請求項の数12 O.L (全 6 頁)

(21)出願番号 特願2000-400839(P2000-400839)

(22)出願日 平成12年12月28日 (2000.12.28)

(71)出願人 501005036

林 利憲
北海道札幌市豊平区平岸1条6丁目3-56

(71)出願人 501005070

山田 康彦
東京都豊島区東池袋4丁目21-5

(71)出願人 501005117

許 先明
埼玉県所沢市寿町20-12

(74)代理人 100101982

弁理士 久米川 正光 (外1名)

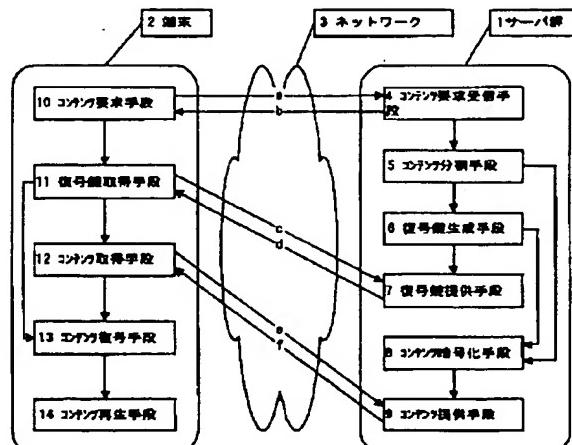
最終頁に続く

(54)【発明の名称】 コンテンツ配信装置、コンテンツ配信方法、コンテンツダウンロードプログラム、コンテンツダウンロード装置

(57)【要約】

【課題】デジタルコンテンツ配信において、正当なユーザーの利便性を損なうことなくコンテンツの不正な複製・流通を防止できる配信方法や配信装置を提供することを目的とする。

【解決手段】サーバに蓄積されたデジタルコンテンツを二つ以上の部分に分割するとともに、そのそれぞれについて異なる暗号鍵によって暗号化し、分割されたデジタルコンテンツを暗号化した状態でユーザに配信するとともに、配信した分割デジタルコンテンツに適用可能な復号鍵をユーザに配信することを特徴とする、デジタルコンテンツ配信方法。



【特許請求の範囲】

【請求項1】デジタルコンテンツをネットワークを介して送信するためのコンテンツ配信装置であって、ユーザからのコンテンツ要求を受信する要求受信手段と、要求されたコンテンツを二つ以上のコンテンツ部分に分割する分割手段と、異なる暗号鍵で暗号化された前記コンテンツ部分をユーザに対して送信する提供手段と、を含む、コンテンツ配信装置。

【請求項2】前記コンテンツ部分のそれに対応する暗号鍵と複合鍵を生成する鍵生成手段を含む、請求項1のコンテンツ配信装置。

【請求項3】前記鍵生成手段によって生成した復号鍵をユーザに対して送信する鍵提供手段を含む、請求項1又は請求項2のコンテンツ配信装置。

【請求項4】前記鍵生成手段によって生成した暗号鍵によって、前記コンテンツ部分のそれを暗号化する暗号手段を含む、請求項1乃至請求項3のコンテンツ配信装置。

【請求項5】デジタルコンテンツをネットワークを介して送信するコンテンツ配信方法であって、ユーザからのコンテンツ要求を受信する要求受信ステップと、要求されたコンテンツを二つ以上のコンテンツ部分に分割する分割ステップと、異なる暗号鍵で暗号化された前記コンテンツ部分をユーザに対して送信するコンテンツ提供ステップと、を含む、コンテンツ配信方法。

【請求項6】デジタルコンテンツをネットワークを介して送信するコンテンツ配信方法であって、ユーザからのコンテンツ要求を受信する要求受信ステップと、

要求されたコンテンツを二つ以上のコンテンツ部分に分割する分割ステップと、前記コンテンツ部分のそれに対応する暗号鍵を生成するステップと、異なる暗号鍵で暗号化された前記コンテンツ部分をユーザに対して送信するコンテンツ提供ステップと、を含む、コンテンツ配信方法。

【請求項7】デジタルコンテンツをネットワークを介して送信するコンテンツ配信方法であって、ユーザからのコンテンツ要求を受信する要求受信ステップと、

要求されたコンテンツを二つ以上のコンテンツ部分に分割する分割ステップと、前記コンテンツ部分のそれに対応する暗号鍵と復号鍵を生成するステップと、異なる暗号鍵で暗号化された前記コンテンツ部分をユーザに対して送信するコンテンツ提供ステップと、

前記部分コンテンツ毎の復号鍵をユーザに対して送信する復号鍵送信ステップと、を含む、コンテンツ配信方法。

【請求項8】サーバからデジタルコンテンツをダウンロードするためのコンテンツダウンロードプログラムであって、暗号化されたデジタルコンテンツの一部である部分コンテンツを受信する手段と、

前記部分コンテンツを復号する復号鍵を受信する手段と、

前記部分コンテンツに対し、前記復号鍵を適用する手段と、を含む、コンテンツダウンロードプログラム。

【請求項9】請求項8に係るコンテンツダウンロードプログラムを格納したコンテンツダウンロードプログラム記録媒体。

【請求項10】サーバからデジタルコンテンツをダウンロードするためのコンテンツダウンロード装置であって、暗号化されたデジタルコンテンツの一部である部分コンテンツを受信する手段と、

前記部分コンテンツを復号する復号鍵を受信する手段と、

前記部分コンテンツに対し、前記復号鍵を適用する手段と、を含む、コンテンツダウンロード装置。

【請求項11】サーバに蓄積されたデジタルコンテンツをユーザに配信する方法であって、

前記デジタルコンテンツを二つ以上の部分に分割するとともに、そのそれについて異なる暗号鍵によって暗号化し、分割された前記デジタルコンテンツを暗号化した状態でユーザに配信するとともに、配信した前記分割されたデジタルコンテンツに適用可能な復号鍵をユーザに配信することを特徴とする、デジタルコンテンツ配信方法。

【請求項12】サーバに蓄積されたデジタルコンテンツを受信する方法であって、

二つ以上の部分に分割された前記デジタルコンテンツの一部であり、独自の暗号鍵で暗号化された分割コンテンツを受信するとともに、前記分割コンテンツに適用可能な復号鍵を受信し、前記分割コンテンツに前記復号鍵を適用することを特徴とする、デジタルコンテンツ受信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、デジタルコンテンツをネットワーク上で販売する際に好適な著作権保護手法に関するものである。本発明は、特に、デジタルコンテンツをネットワーク上で販売する際のコンテンツ配信の際に、必要な不正アクセス防止手法に係るものである。

【従来の技術】デジタルコンテンツをネットワーク上で取引する際にコンテンツの著作権を保護する方法として、コンテンツを暗号化しその再生に専用の解読ソフトを用い、解読の際に特定のパスワード等の鍵情報を用いる方法（例えば、音楽配信に使用されるSDMI（Secure Digital Music Initiative）規格と呼ばれる手法や世の中で有料放送で行われているスクランブル放送の手法が知られている）や、解読の際に所定の情報鍵をネットワーク上の鍵センタより取得し当該鍵を用いてコンテンツの復号・再生を行う方法等が考えられる。

【0003】前者の方法では、コンテンツの不正な流通、利用を完全に防止できず、またコンテンツの正当なユーザーの利便性をも損なうという問題があった。例えば、コンテンツをユーザー毎の暗号鍵を用いて、コンテンツを暗号化した上でデータを圧縮し、これをネットワークを介してユーザー側の端末に配達し、同時にダウンロードした対となる解読用の復合鍵を用いて、専用プレーヤー又はソフトウェアを用いて再生するという方法がこの方法の典型的な運用方法である。しかし、この方法では、特定の専用プレーヤー又はソフトウェアを用いることが復号の条件なので、専用プレーヤー又はソフトウェアが利用できない環境下（例えば、自宅以外の場所など）においては、著作権の利用権限を有する正当なユーザーであっても、使用する端末（プレーヤーも含めて）によっては再生が不可能になる等、コンテンツユーザーの利便性を損なうという問題があった。

【0004】後者の方法は、情報鍵を鍵センタより取得するため、特定の端末でないとコンテンツが利用できないという問題は解消され、ユーザーの利便性を損なうことはない。しかし、所定の鍵を用いるため、鍵自身が不正にアクセスされて、流出したときには、コンテンツの不正な流通、利用を完全に防止できない。

【0005】

【発明が解決しようとする課題】そこで、本発明は、デジタルコンテンツの配信において、正当なユーザーの利便性を損なうことなくコンテンツの不正な複製・流通を防止できる配信方法や配信装置を提供することを目的とするものである。

【0006】

【課題を解決するための手段】前記課題を解決するため、本発明では、配信時にサーバ群上のコンテンツを任意の単位として分割することを特徴とする、デジタルコンテンツをネットワークに接続されたユーザーの端末上で再生可能とするコンテンツの配信方法を提供する。

【0007】より具体的にいうと、本発明は、サーバに蓄積されたデジタルコンテンツをユーザーに配信する方法であって、デジタルコンテンツを二つ以上の部分に分割するとともに、そのそれぞれについて異なる暗号鍵によって暗号化し、分割されたデジタルコンテンツを暗号化した状態でユーザーに配信するとともに、配信した分割デ

ジタルコンテンツに適用可能な復号鍵をユーザーに配信することを特徴とする、デジタルコンテンツ配信方法を提供するものである。このような方法で分割・暗号化・配信されたコンテンツについて、ユーザーは分割コンテンツを受信するステップと、分割コンテンツを受信すると同時に前記暗号鍵に対応する復号鍵をネットワークを通じて取得するステップと、前記復号鍵を用いて前記分割コンテンツを復号するステップと、前記分割コンテンツと前記復号鍵を削除するステップを繰り返すことによって、コンテンツ全体の配信を行うことを特徴とする。

【0008】より具体的にいうと、ユーザーについては、本発明は、サーバに蓄積されたデジタルコンテンツを受信する方法であって、二つ以上の部分に分割された前記デジタルコンテンツの一部であり、独自の暗号鍵で暗号化された分割コンテンツを受信するとともに、分割コンテンツに適用可能な復号鍵を受信し、分割コンテンツに前記復号鍵を適用することを特徴とする、デジタルコンテンツ受信方法として説明することができる。

【0009】本発明に係る解決手段をさらに説明すると、例えば、以下のようなになる。即ち、本発明は、デジタルコンテンツをネットワークを介して送信するためのコンテンツ配信装置であって、ユーザーからのコンテンツ要求を受信する機構と、要求されたコンテンツを二つ以上のコンテンツ部分に分割する機構と、異なる暗号鍵で暗号化されたコンテンツ部分をユーザーに対して送信する機構と、を含むものである。

【0010】本発明は、さらに、コンテンツ部分のそれぞれに対応する暗号鍵と複合鍵を生成する鍵生成機構、鍵生成手段によって生成した復号鍵をユーザーに対して送信する鍵提供機構、鍵生成手段によって生成した暗号鍵によって、コンテンツ部分のそれぞれを暗号化する暗号化機構のいずれか一つ又は二つ以上を含むものであっても構わない。

【0011】また、本発明は、デジタルコンテンツをネットワークを介して送信するコンテンツ配信方法であって、ユーザーからのコンテンツ要求を受信する要求受信ステップと、要求されたコンテンツを二つ以上のコンテンツ部分に分割する分割ステップと、異なる暗号鍵で暗号化された前記コンテンツ部分をユーザーに対して送信するコンテンツ提供ステップと、を含むものである。このコンテンツ配信方法は、コンテンツ部分のそれぞれに対応する暗号鍵を生成するステップ、若しくは、コンテンツ部分のそれぞれに対応する暗号鍵及び復号鍵を生成するステップを含むものであっても構わない。

【0012】また、本発明をユーザーの使用するプログラムという形で示すと以下のようになる。即ち、本発明は、サーバからデジタルコンテンツをダウンロードするためのコンテンツダウンロードプログラムであって、暗号化されたデジタルコンテンツの一部である部分コンテンツを受信する機構と、部分コンテンツを復号する復号

鍵を受信する機構と、部分コンテンツに対し、復号鍵を適用する機構と、を含むものである。

【0013】

【発明の実施の形態】以下、図面を参照して本発明のコンテンツの配信方法の実施の形態の一例を説明する。

【0014】図1は本実施の形態におけるシステムの概略構成を示すもので、1はサーバ群、2はパーソナルコンピュータ等で構成される複数の端末、3はこれらを任意に接続するネットワークである。ここで、配信しようとする、デジタルコンテンツは、サーバ群1上に格納されているものとする。

【0015】また、図2は前記システムにおける要部構成を示す。サーバ群1はコンテンツ要求受信手段4、コンテンツ分割手段5、復号鍵生成手段6、復号鍵提供手段7、コンテンツ暗号化手段8、コンテンツ提供手段9を備えている。また、各端末2はコンテンツ要求手段10、復号鍵取得手段11、コンテンツ取得手段12、コンテンツ復号手段13及びコンテンツ再生手段14を備えている。なお、これらの各手段はサーバ群1及び端末2をそれぞれ構成するコンピュータとそのプログラムによって実現される。

【0016】サーバ群1に備えられた各手段の機能と本発明の実現スキームについて説明する。

【0017】コンテンツ要求受信手段4は端末2からのコンテンツ要求を受信する。このコンテンツ要求を受けて、端末2に対して、コンテンツ要求を受領した旨を返信するとともに、コンテンツ分割手段5が配達すべきコンテンツを任意の単位数に分割する。この分割されたコンテンツのことを以降、「分割コンテンツ」という。復号鍵生成手段6はコンテンツ分割手段5により分割された分割コンテンツ毎に復号鍵を生成する。復号鍵提供手段7は、端末2からの要求に応じて、復号鍵生成手段6により生成された復号鍵をネットワーク3を介して該端末2に提供する。

【0018】コンテンツ暗号化手段8はコンテンツ分割手段5により分割された分割コンテンツを鍵生成手段6により生成された暗号化鍵により暗号化する。コンテンツ提供手段9はコンテンツ暗号化手段8により暗号化された分割コンテンツを端末2からの要求に応じてネットワーク3を介して該端末2に提供する。

【0019】次に、本発明の実現スキームとサーバ群1・端末2間の通信スキームについて簡単に説明する。

【0020】① コンテンツ要求手段10はネットワーク3を介してサーバ群1との通信を実現し、端末2におけるユーザのコンテンツ再生命令をサーバ群1に送信する。メッセージaは再生命令に係るコンテンツを指定する情報を含む。また、これに応じて、コンテンツ要求受信手段は、要求されたコンテンツの分割情報を含むメッセージbを返信する。ここで、コンテンツの分割情報bは、分割されたコンテンツを元に戻すために必要な情報

のことをいい、例えば、コンテンツ全体のサイズ、分割単位の大きさ、圧縮手法、暗号化の手法、分割されたコンテンツの順序を含む。

【0021】② 復号鍵取得手段11はネットワーク3を介してサーバ群1との通信を実現し、復号鍵をサーバ群1から取得する。ここで、メッセージcは対応する鍵が必要な分割コンテンツを指定する情報を含み、メッセージdは復号鍵を含むメッセージである。

【0022】③ コンテンツ取得手段12はネットワーク3を介してサーバ群1との通信を実現し、分割コンテンツをサーバ群1から取得する。ここで、メッセージeは必要な分割コンテンツを指定する情報を含み、メッセージfは分割コンテンツそれ自体を含むメッセージである。

【0023】④ コンテンツ復号手段13は、コンテンツ取得手段12により取得した分割コンテンツを復号鍵取得手段11により取得した復号鍵を用いて復号し、復号鍵を削除する。コンテンツ再生手段14は、コンテンツ復号手段13により復号された分割コンテンツの再生、削除を行う。

【0024】以下、このスキームについて、さらに詳細な説明を加える。

【0025】前記構成において、ユーザが端末2を利用して、特定のコンテンツの再生を命じるとコンテンツ要求手段10が起動し、ネットワーク3を介して、前記コンテンツを指定するメッセージaをサーバ群1に送る。メッセージaを受け取ったサーバ群1は、コンテンツ要求受信手段4を起動し、コンテンツ要求受信手段4は、メッセージaからコンテンツを指定する情報を取り出す。このコンテンツ指定情報は、コンテンツ分割手段5に送られ、対応するコンテンツの分割情報を含むメッセージbがサーバ群1からネットワーク3に返送される。コンテンツ分割手段5は、指定されたコンテンツの分割を行う。コンテンツ分割手段5は分割コンテンツをコンテンツ暗号化手段8に送るとともに、復号鍵生成手段6に暗号鍵の生成を命じる。

【0026】復号鍵生成手段6は分割コンテンツ毎に対応する暗号鍵を生成し、生成した暗号鍵を復号鍵提供手段7及びコンテンツ暗号化手段8に送る。

【0027】ネットワーク3を介してメッセージbを受け取った端末2のコンテンツ要求手段10はメッセージbからコンテンツの分割情報を取り出し復号鍵取得手段11に送る。

【0028】復号鍵取得手段11は、どの分割コンテンツに対応する鍵が必要であるかを指定するメッセージcをネットワーク3を介して、複合鍵提供手段7に送る。ネットワーク3を介してメッセージcを受け取ったサーバ群1の復号鍵提供手段7は、復号鍵を含むメッセージdをネットワーク3に返送する。

【0029】コンテンツ暗号化手段8はコンテンツ分割

手段5より受け取った分割コンテンツを復号鍵生成手段6より受け取った前記分割コンテンツに対応する暗号化鍵を使用して暗号化し、暗号化した分割コンテンツをコンテンツ提供手段9に送る。

【0030】ネットワーク3を介してメッセージdを受け取った端末2の復号鍵取得手段11は復号鍵情報を取り出しコンテンツ復号手段13に送り、コンテンツ取得手段12に分割コンテンツの取得を命じる。

【0031】コンテンツ取得手段12は必要な分割コンテンツを指定するメッセージeをネットワーク3に送る。ネットワーク3を介してメッセージeを受け取ったサーバ群1のコンテンツ提供手段9は該当する分割コンテンツを含むメッセージfをネットワーク3に返送する。

【0032】ネットワーク3を介してメッセージfを受け取った端末2のコンテンツ取得手段12は分割コンテンツを取り出しコンテンツ復号手段13に送る。

【0033】コンテンツ復号手段13はコンテンツ取得手段12より受け取った分割コンテンツを復号鍵取得手段11より受け取った復号鍵により復号し、コンテンツ再生手段14に送り、復号鍵を削除する。

【0034】コンテンツ再生手段14はコンテンツ復号手段13より受け取ったコンテンツを再生し削除する。

【0035】以下同様に、コンテンツ終了まで復号鍵取得手段11以降の手順を繰り返す。本明細書において述べた端末2に係るコンテンツ受信手段10、複合鍵取得手段11、コンテンツ取得手段12、コンテンツ複合手段13、コンテンツ再生手段14並びにサーバ群1に係るコンテンツ要求受信手段4、コンテンツ分割手段5、複合鍵生成手段6、複合鍵提供手段7、コンテンツ暗号*30

*化手段8、コンテンツ提供手段9ともに、ハードウェアを用いて構成しても、ソフトウェアを用いて構成しても、あるいは、ハードウェアとソフトウェアを用いて構成してもよい。また、ネットワーク3は、公開されたインターネットに限らず、非公開のネットワークやLAN等を用いても本発明に適用することができ、さらに、有線・無線を問うものではない。

【0036】

【発明の効果】以上説明したように、本発明によればデジタルコンテンツの配信において、正当なユーザの利便性を損なうことなくコンテンツの不正な複製・流通を防止できる。

【0037】また、万一の鍵が流出したとしても分割された単位コンテンツにとどまるため、コンテンツ全体を利用することはできない。よって、不正な流通、利用を効果的に防止することが可能である。

【0038】また、サーバ群からの復号鍵の取得にあって、ユーザ側より当該鍵の暗号化鍵をサーバ群へ送信し、サーバ群側からは当該暗号鍵で暗号化したコンテンツ復号鍵を送出することによって、ネットワーク経路上における鍵の流出を強力に防止できる。

【図面の簡単な説明】

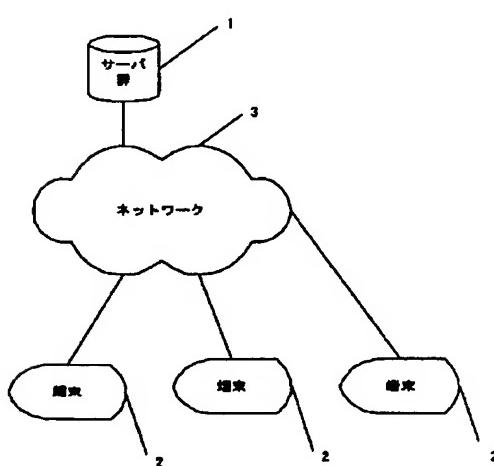
【図1】本発明が適用されるシステムを示す図である。

【図2】本発明が適用される端末とサーバ群の構成を示す図である。

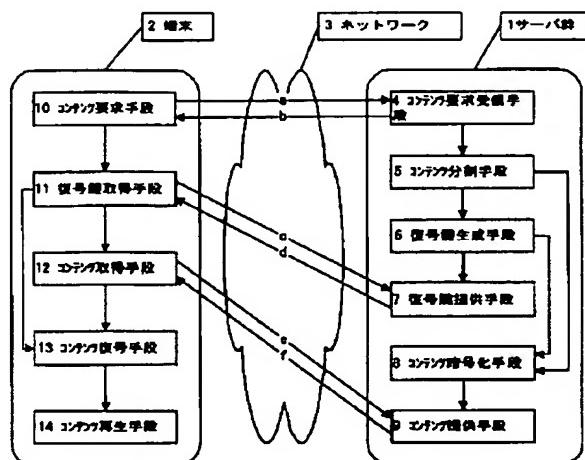
【符号の説明】

- 1 サーバ群
- 2 端末
- 3 ネットワーク

【図1】



【図2】



フロントページの続き

(71)出願人 501005058
中原 順志
東京都杉並区松ノ木3-33-29
(72)発明者 林 利憲
札幌市豊平区平岸1条6丁目3-56
(72)発明者 山田 康彦
東京都豊島区東池袋4丁目21-5

(72)発明者 許 先明
埼玉県所沢市寿町20-12
(72)発明者 中原 順志
東京都杉並区松ノ木3-33-29
F ターム(参考) 5B085 AE13 AE29 CA04
SJ104 AA01 AA16 AA34 EA01 EA04
EA16 NA02 PA07